UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/466,625	12/17/1999	RONALD P. DOYLE	RSW990077	1396

7590 10/09/2003

JEANINE S RAY-YARLETTS
IBM CORP DEPT T81/BLDG 062
PO BOX 12195
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER	
WU, ALLEN S	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/09/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/466,625	DOYLE ET AL.	
	Examiner	Art Unit	
	Allen S. Wu	2131	

-- Th MAILING DATE of this communication appears on th cover she t with th correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 December 1999* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: 600, 610, 620, 630, 640, 650, 670, 680 in fig. 6. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

2. Claims 8, 9, 17, 18, 26 and 27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claims 8, 9, 17, 18, 26, and 27 recites the limitation "said generated passticket" in the last 2 lines of each claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 7, 9, 10, 16, 18, 19, 25, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kung, US Patent 5,241,594 in view of Brezak, Jr. et al, US Patent 6,401,211, and further in view of Devine et al, Patent Application number 09/159,514.

As per claim 1, 10, and 19, Kung discloses a computer program, method and system for user authentication of network access (abstract), which comprises of computer-readable program code means for establishing a secure session from a client machine to a server machine (secure transport layer protocol, col 3 ln 25-33; communication between the workstation and a multiple logon server, fig 2 and col 4 ln 30-48) using user identification data (user ID and password, col 4 ln 30-48); storing user identification information at the server (system having a central server on which the Ids and encrypted passwords are stored, col 2 ln 50-55). Kung does not teach passing user identification information from server machine to a host access security system. Brezak, Jr. et al teaches a host access security system (Kerberos Key Distribution Center, col 5 ln 54-67 and col 6 ln 1-12). Communication between a server and a user's computer is the same as communication between a host and a server in a network. This is because a computer can act as a host or a server. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the host access security system of Brezak, Jr. et al within the system of Kung because it would have added an extra layer of authentication and further security to the user logon process of Kung. Using a host access

security system provides a more efficient and secure method of authenticating the user and providing access information based on user credentials.

Kung further discloses accessing a stored password representing user id (user id and password stored on server are employed, col 4 ln 40-48). Kung does not teach accessing a generated password substitute. However, Brezak, Jr. et al teaches accessing a generated password substitute (ticket granting ticket, col 5 ln 54-67 and col 6 ln 1-37). A password and a generated password substitute both consist of digital information used for user or machine authentication. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the generated password substitute within the system of Kung because it would have eliminated the need for the user to remember or create a password.

Furthermore, Kung does not teach the password or a generated password substitute representing located credentials. Brezak Jr. et al teaches accessing a generated password substitute (ticket granting ticket, col 5 ln 54-67 and col 6 ln 1-37) representing user access credentials (user's credentials to authenticate user, col 6 ln 19-21; directory service for the account data of user, col 6 ln 23-30). A password or stored generated password substitute can represent anything, including the user id or user access credentials. Storing the password is the same as storing digital data, which can represent any attribute. It would have been obvious to one of ordinary skill in the art to combine the teachings of Brezak, Jr. et al within the system of Kung because it would have provided an

extra layer of security. Accessing stored password or generated password substitute representing located user credentials ensures that the password is associated with the user requesting the information.

Furthermore, Kung discloses using stored password to transparently log user on to a secure host application executing at host system (user ID and password are employed to logon to host automatically, col 4 ln 40-48). The combination of Kung and Brezak, Jr. et al does not teach the host application being a legacy host application. However, Devine et al teaches communication to a legacy host system (Abstract, fig 1, page 5 paragraph 70). Legacy host applications serve the same as any host application, except that it may be based off of prior systems or code. Extending communication to legacy host applications requires modifying protocols to be able to communicate with legacy systems. The legacy systems are common in enterprise systems. It would have been obvious to one of ordinary skill in the art to combine the legacy host system of Devine et al within the combination of Kung and Brezak, Jr. et al because it would have allowed the legacy host applications to authenticate a user without requiring the user to enter a user id and password for each application requesting access.

Furthermore, the combination of Kung and Brezak, Jr. et al do not teach communication protocol being a legacy host communication protocol. However, Devine et al teaches communication to a legacy host system (Abstract, fig 1, page 5 paragraph 70; Devine et al does not explicitly state any legacy host

communication protocol. Devine et al discloses a system for legacy host system. Any communication protocol disclosed is inherently a protocol for use with legacy host systems). Communication protocols are necessary in networks to communicate between different hosts, servers, clients, and the like. A legacy host communication protocol serves the same purpose of any communication protocol, except legacy host communication protocols provide communication to legacy hosts. It would have been obvious to one of ordinary skill in the art to combine the teachings of Devine et al within the combination of Kung and Brezak, Jr. et al because it would have allowed for communication to legacy hosts. Communication to legacy hosts are important in that most enterprise systems consist of legacy hosts, allowing users more capability to access different applications and data.

The combination Kung and Brezak, Jr. et al do not teach user identification data being a digital certificate. Devine et al teaches the use of digital certificates for authentication (server will send a digital certificate....optionally request a certificate from the client, page 7 paragraph 88). Digital certificates serve the same purpose of password and user id combinations. Both are used for the purpose of authenticating a user or machine. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the digital certificate of Devine et al. within the combination of Kung and Brezak Jr. et al because it would have added a more secure authentication algorithm. Using digital certificates does not require

the user to remember any passwords and less likely to be stolen and used by outsiders.

As per claims 7, 16, and 25, Kung teaches a server (multiple logon server, fig 1 col 6 ln 51-60). The combination of Kung and Brezak, Jr. et al does not teach the server machine being a Web application server machine. However, Devine et al discloses a web server to provide user sessions (secure web server, fig 1, page 3 paragraph 51-52). A server can be any computer that provides services to other computer programs or users. A web application server machine is a computer that serves web applications to users and is well known in the art. It would have been obvious to one of ordinary skill in the art to combine the teachings of Devine et al within the combination of Kung and Brezak, Jr. because it would have allowed users to transparently log on to web applications.

As per claims 9, 18, and 27, Kung teaches the host application (remote host computer, col 5 ln 7-18) to request log on information for the user (requests entry of a user ID and password, col 5 ln 7-18). Responding by supplying a user identifier (user id codes, col6 ln 51-60) associated with a stored password (encrypted passwords, col 6 ln 51-60). Kung does not teach a user identifier associated with located access credentials. Brezak Jr. et al teaches accessing a generated password substitute (ticket granting ticket, col 5 ln 54-67 and col 6 ln 1-37) representing user access credentials (user's credentials to authenticate

user, col 6 ln 19-21; directory service for the account data of user, col 6 ln 23-30). Incorporating access credentials associated with a user id is the same as the use of passwords associated with a user id. Both are stored and processed as digital data. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Brezak Jr. et al within the system of Kung because it would have provided an extra layer of security. The system can authenticate the user with the password, and at the same time, use the user id to check for access privileges of the user.

6. Claims 3-5, 12-14, and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kung, US Patent 5,241,594 in view of, Brezak, Jr. et al, US Patent 6,401,211, further in view of Devine et al, Patent Application number 09/159,514, as applied to claims 1, 10, and 19 above, and further in view of Butts et al, US Patent 5,754,830.

As per claims 3, 12, and 21, the combination of Kung, Brezak, Jr. et al, and Devine et al does not teach a 3270 emulation protocol. However, Butts et al discloses a 3270 terminal session for communication between legacy host systems (col 5, ln 44-52 and col 6 ln 22-27; A 3270 terminal session has to use 3270 emulation protocol for communication purposes. Therefore, the 3270 emulation protocol is inherent to the invention of Butts et al). Communication protocols are some way of passing digital information between two machines. The use of a 3270 emulation protocol can be a more efficient protocol than

others, depending on the network system used and is well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the 3270 emulation protocol within the combination of Kung, Brezak, Jr. et al, and Devine et al because it would have provided a more reliable and efficient communication protocol to exchange information between systems on a network.

As per claims 4, 13, and 22, the combination of Kung, Brezak, Jr. et al, and Devine et al does not teach a 5250 emulation protocol. However, Butts et al discloses a 5250 terminal session for communication between legacy host systems (col 5, ln 44-52 and col 6 ln 22-27; A 5250 terminal session has to use 5250 emulation protocol for communication purposes. Therefore, the 5250 emulation protocol is inherent to the invention of Butts et al). Communication protocols are some way of passing digital information between two machines. The use of a 5250 emulation protocol can be a more efficient protocol than others, depending on the network system used and is well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the 5250 emulation protocol within the combination of Kung, Brezak, Jr. et al, and Devine et al because it would have provided a more reliable and efficient communication protocol to exchange information between systems on a network.

As per claims 5, 14, and 23, Kung discloses a virtual terminal protocol (TELNET, col 4 ln 60-67; Kung does not explicitly state a virtual terminal protocol. TELNET is a virtual terminal, which uses virtual terminal protocols that is well known in the art. Therefore, a virtual terminal protocol is to be inherent to the invention of Kung).

7. Claims 6/1, 15/10, and 24/19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kung, US Patent 5,241,594 in view of, Brezak, Jr. et al, US Patent 6,401,211, further in view of Devine et al, Patent Application number 09/159,514, further in view of Butts et al, US Patent 5,754,830 as applied to claims 3/1, 12/10, and 21/19 above, and further in view of Guski et al, US Patent 5,592,553.

As per claims 6/1, 15/10, and 24/19, Kung teaches a host access security system (Kerberos Key Distribution Center, col 5 ln 54-67 and col 6 ln 1-12). The combination of Kung, Brezak, Jr. et al, Devine et al, and Butts et al does not teach the host access security system being a Resource Access Control Facility (RACF) system. Guski et al teaches the use of Resource Control Facility to authenticate a user (col 6, ln 42-56). Host access security systems provide access to authorized users through manipulating or comparing digital data. The systems serve the same purpose and only differ in their protocols. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the resource access control facility of Guski et al within the combination of Kung, Brezak, Jr. et al, Devine et al, and Butts et al because

resource access control facility is a more specific and standard form of access security that is well known in the art.

8. Claims 2, 11, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kung, US Patent 5,241,594 in view of, Brezak, Jr. et al, US Patent 6,401,211, further in view of Devine et al, Patent Application number 09/159,514.as applied to claims 1, 10, and 19 above, and further in view of Schneier.

As per claims 2, 11, and 20, Devine et al discloses a digital certificate (server will send a digital certificate....optionally request a certificate from the client, page 7 paragraph 88). However, the combination of Kung, Brezak, Jr. et al, and Devine et al does not teach the digital certificate being an X.509 certificate. Schneier discloses a X.509 certificate for authentication as the ISO authentication framework (pages 574-575). Digital certificates can take many different forms, depending on different protocols, but are still stored as digital data. Their purpose is still to authenticate a user or machine. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Schneier within the combination of Kung, Brezak, Jr. et al, and Devine et al because is would have added better reliability due to the use of an ISO standard certificate.

9. Claims 3/2-5/2, 12/11-14/11, and 21/20-23/20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kung, US Patent 5,241,594 in view of, Brezak, Jr. et al, US Patent No., 6,401,211, further in view of Devine et al, Patent

Application number 09/159,514, further in view of Schneier as applied to claims 2, 11, and 20 above, and further in view of Butts et al, US Patent 5,754,830.

As per claims 3/2, 12/11, and 21/20, the combination of Kung, Brezak, Jr. et al, Devine et al, and Schneier does not teach a 3270 emulation protocol. However, Butts et al discloses a 3270 terminal session for communication between legacy host systems (col 5, ln 44-52 and col 6 ln 22-27; A 3270 terminal session has to use 3270 emulation protocol for communication purposes. Therefore, the 3270 emulation protocol is inherent to the invention of Butts et al). Communication protocols are some way of passing digital information between two machines. The use of a 3270 emulation protocol can be a more efficient protocol than others, depending on the network system used and is well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the 3270 emulation protocol within the combination of Kung, Brezak, Jr. et al, Devine et al, and Schneier because it would have provided a more reliable and efficient communication protocol to exchange information between systems on a network.

As per claims 4/2, 13/11, and 22/20, the combination of Kung, Brezak, Jr. et al, Devine et al, and Schneier does not teach a 5250 emulation protocol. However, Butts et al discloses a 5250 terminal session for communication between legacy host systems (col 5, ln 44-52 and col 6 ln 22-27; A 5250 terminal

session has to use 5250 emulation protocol for communication purposes. Therefore, the 5250 emulation protocol is inherent to the invention of Butts et al). Communication protocols are some way of passing digital information between two machines. The use of a 5250 emulation protocol can be a more efficient protocol than others, depending on the network system used and is well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the 5250 emulation protocol within the combination of Kung, Brezak, Jr. et al, Devine et al, and Schneier because it would have provided a more reliable and efficient communication protocol to exchange information between systems on a network.

As per claims 5/2, 14/11, and 23/20, Kung discloses a virtual terminal protocol (TELNET, col 4 ln 60-67; Kung does not explicitly state a virtual terminal protocol. TELNET is a virtual terminal, which uses virtual terminal protocols that is well known in the art. Therefore, a virtual terminal protocol is to be inherent to the invention of Kung).

10. Claims 6/2, 15/11, and 24/20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kung, US Patent 5,241,594 in view of, Brezak, Jr. et al, US Patent 6,401,211, further in view of Devine et al, Patent Application number 09/159,514, further in view of Schneier, further in view of Butts et al, US Patent 5,754,830 as applied to

claims 3/2, 12/11, and 21/20 above, and further in view of Guski et al, US Patent 5,592,553.

As per claims 6/2, 15/11, and 24/20, Kung teaches a host access security system (Kerberos Key Distribution Center, col 5 ln 54-67 and col 6 ln 1-12). The combination of Kung, Brezak, Jr. et al, Devine et al, Schneier, and Butts et al does not teach the host access security system being a Resource Access Control Facility (RACF) system. Guski et al teaches the use of Resource Control Facility to authenticate a user (col 6, ln 42-56). Host access security systems provide access to authorized users through manipulating or comparing digital data. The systems serve the same purpose and only differ in their protocols. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the resource access control facility of Guski et al within the combination of Kung, Brezak, Jr. et al, Devine et al, Schneier, and Butts et al because resource access facility is a more specific and standard form of access security that is well known in the art.

11. Claims 8, 17, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kung, US Patent 5,241,594 in view of, Brezak, Jr. et al, US Patent 6,401,211, further in view of Devine et al, Patent Application number 09/159,514 as applied to claims 1, 10, and 19 above, and further in view of IBM Technical Disclosure Bulletin, document number NN9204459.

As per claims 8, 17, and 26 Kung teaches the host application (remote host computer, col 5 ln 7-18) to request log on information for the user (requests entry of a user ID and password, col 5 ln 7-18). Responding by supplying a user identifier (user id codes, col 6 ln 51-60) associated with a stored password (encrypted passwords, col 6 ln 51-60). The combination of Kung, Brezak, Jr. et al and Devine et al does not teach the logon message having placeholders representing the user identification and a password. However, the IBM technical disclosure discloses placeholders in messages (description text may contain placeholder symbols %s...the %s symbols are replaced by error arguments, see disclosure text). Placeholders are used to pass parameters between different machines or modules. The user identifier is a parameter to the log on message and consists of digital data. Error arguments in the IBM technical disclosure also consist of digital data. In both situations, the placeholder is used to hold the place for a parameter, so that the parameters can be passed between different machines or modules. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of the IBM technical disclosure within the combination of Kung, Brezak, Jr. et al, and Devine et al because it would have allowed the use of the combination with different logon messages. If each logon message has a different format, the use of placeholders tells the server where to put the parameter needed, the user identification data, so that the host can extract the data correctly.

Furthermore, the combination of Kung, Brezak, Jr. et al, and Devine et al does not teach substituting a user identifier associated for the placeholders. The IBM technical disclosure teaches substituting parameters for the placeholders (%s symbols are replaced by the error arguments, see disclosure text). According to the IBM technical disclosure, placeholders are used to pass parameters to machines or modules. User identification data and error arguments both consist of digital data. In both situations, the placeholder is used to hold the place for a parameter, so that the parameters can be passed between different machines or modules. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of the IBM technical disclosure within the combination of Kung, Brezak, Jr. et al, and Devine et al because it would have allowed the use of the combination with different logon messages. If each logon message has a different format, the substituting the parameter needed, user identification, for the placeholders allows the host can extract the data according to its own logon format.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Richard et al, US Patent 5,922,074 discloses accessing user credentials list corresponding using a user's digital certificate.

He, Patent Number 5,944,824 discloses the use of a generated random password and ticket to authenticate users.

Jones et al, US Patent 5,655,077, discloses single sign on scheme, which transparently logs on users to different computing services.

Wray et al., US Patent 6,442,696, discloses using digital certificates to authenticate and transparently log on users.

Davis et al, Computer Networks and Their Protocols, discloses different communication protocols including virtual terminal protocols.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-0900.

Allen S. Wu
Examiner
Art Unit 2131

ASW

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100